PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32 — A1

(11) International Publication Number: WO 99/37055

(43) International Publication Date: 22 July 1999 (22.07.99)

(21) International Application Number: PCT/US99/00778

(22) International Filing Date: 14 January 1999 (14.01.99)

(30) Priority Data:
09/008,527 16 January 1998 (16.01.98) US

(63) Related by Continuation (CON) or Continuation-in-Part (CIP) to Earlier Application
US 09/008,527 (CON)
Filed on 16 January 1998 (16.01.98)

(71) Applicant *(for all designated States except US)*: AMERITECH CORPORATION [US/US]; 2000 W. Ameritech Center Drive, Hoffman Estates, IL 60196–1025 (US).

(72) Inventors; and

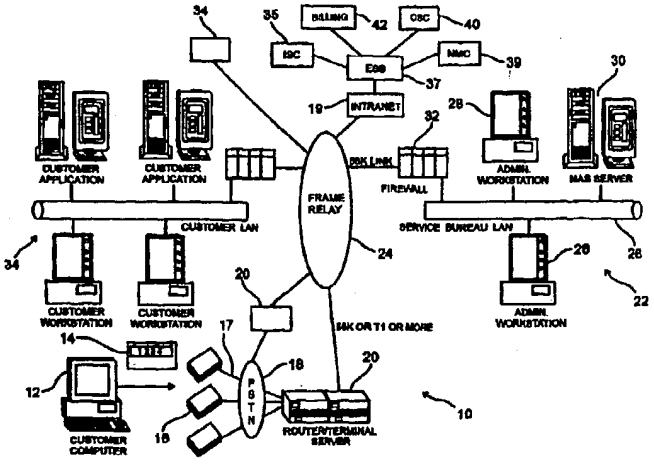
(75) Inventors/Applicants *(for US only)*: TIANEN, Carl, Richard [US/US]; 36270 Mallory Court, Livonia, MI 48150 (US). IRISH, Terry, Robert [US/US]; Apartment 6, 8010 Deepwood Boulevard, Mentor, OH 44060 (US). CARROLL, Barbara, Miller [US/US]; 9704 Bonner Lane, Spring Grove, IL 60081–8820 (US). WOODS, Donna, Kay [US/US]; 3671 Ronald Road, Crete, IL 60417–1605 (US). EATON, Philip, Robert [US/US]; Apartment B, 9416 Kungsholm Drive, Indianapolis, IN 46250–1141 (US). GRANGER, Craig, Michael [US/US]; 4071 Lotus Drive, Waterford, MI 48329 (US). MASSEL, James, William [US/US]; 10630 Tennison Drive, Indianapolis, IN 46236 (US).

(74) Agent: GENIN, Kent, E.; Brinks Hofer Gilson & Lione, P.O. Box 10087, Chicago, IL 60610 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: SYSTEM AND METHOD FOR PROVIDING SECURE REMOTE ACCESS TO A COMPUTER NETWORK



BEST AVAILABLE COPY

(57) Abstract

A system (fig. 1) for providing secure remote access for a plurality of host computer networks and their respective authorized users includes a network access server operated by a third party service provider for authenticating users based on identifying information provided by each remotely located user. A method is disclosed wherein the network access server (fig. 3, #30) authenticates remote users (fig. 3, #12) and establishes a communication link between an appropriate one of the plurality of host computer networks utilizing the network access server for remote access authentication of the remote users associated with each subscribing host computer network.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

SYSTEM AND METHOD FOR PROVIDING SECURE REMOTE ACCESS TO A COMPUTER NETWORK

BACKGROUND OF THE INVENTION

The present invention relates to a method and apparatus for providing remote secure access to computer networks. More particularly, the present invention relates to a method and apparatus for securing communications between remotely located workers and the appropriate destination computer through a single, off-site security server.

Many organizations, both in government and in private industry, rely on access to centralized computer facilities. Ease of access is generally desirable in order to facilitate use of computer resources and productivity. Remotely located individuals who are, for example, traveling on business, often need to access their organization's computer. A concern for each organization is that access only be granted to the appropriate personnel.

One approach to addressing this security issue is for each organization to have a security system or infrastructure that is specific to the organization. Each company would, for example, receive modem calls from its remotely located employees and process the call through some type of password routine or other verification process. Maintaining adequate and current security measures can be a burden both in the amount of dedicated hardware and in the amount of software that must be managed. Proper security may be beyond the means of smaller organizations and may take up considerable resources for larger organizations.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a remote access system according to a preferred embodiment of the invention.

FIG. 2 is a block diagram of a preferred communication server for use in the system of FIG. 1.

FIG. 3 is a block diagram of a preferred network access server for use in the system of FIG. 1.

FIG. 4 is a flow diagram illustrating a preferred method of establishing secure computer access between a remote user and the appropriate computer system.

DETAILED DESCRIPTION OF PRESENTLY PREFERRED EMBODIMENTS

According to one aspect of the present invention an improved method and apparatus for securing computer access between users and the proprietary computer network of each user's respective organization is provided. The preferred system and method are advantageous in that they reduce the infrastructure and overhead burden on individual organizations by removing the task of authenticating users, and associated administrative tasks, to an off-site security system managed by a third party service provider.

FIG. 1 illustrates a preferred system 10 for securing access between remotely located computer users and the computers of the different organizations that they are permitted to access. The system 10 includes at least one remotely located user computer 12. Preferably, there are multiple remotely located user computers 12. A security token, for example a secure identification card 14, is associated with each user. Each user preferably communicates through her user computer 12 over standard telephone lines, also known as plain old telephone service (POTS) lines 17, via modem 16 through the public switched telephone network (PSTN) 18. At least one communication server 20, which may be a router such as a Cisco 5200, is in communication with a security service bureau 22 over a frame relay network 24. The security service bureau 22 may be a local area network (LAN) 26 that includes at least one administrative workstation 28 for monitoring operation of the security service bureau 22. A suitable administrative workstation 28 may be any of a number of commonly available personal computers. A network access server (NAS) 30 is also connected to the LAN 26. The LAN 26 of the service bureau 22 connects to the frame relay network 24 through a fire wall 32. The fire wall may be a personal computer, such as those available from Sun Microsystems, running software available

from Solaris to provide protection to the service bureau LAN 26 from outside corruption. The NAS 30 may be any of a number of servers such as those available from Hewlett Packard, including the HP 712, the HP 755, or the HP 720. Similar devices from other manufacturers may also be used as the NAS. The NAS 30 of the service bureau 22 is in communication with multiple host computer networks 34 or stand-alone computers over the frame relay network 24. In the example of FIG. 1, each of the host computer networks or stand-alone computers utilize the service bureau to authenticate remote users at various computers 12. As used below, the term host computer network refers to the computer, computer system, or group of computer systems operated by an organization such as a business or corporation. Preferably, each of the plurality of host computer networks 34 is operated by a separate, unrelated organization.

The system 10 also includes an integrated service center (ISC) 35 and an enterprise service system (ESS) 37. The ISC 35 preferably includes a computer configured to accept all service requests from host computer networks desiring to add or remove computer use monitoring services or change the list of authorized users for the network. Additionally, the ISC 35 receives telephone calls from end users 12 seeking help relating to remote access services. The ISC 35 assigns help requests to the appropriate party in the system 10. In one embodiment, the ISC 35 is a vertically integrated service center and help desk for video, audio, and data communications.

The ESS 37 is a master database containing lists of periodic user charges, also known as "per seat" charges, for the various host computer systems serviced by the system 10. The ESS 37 also contains a list of field service fees associated with a respective host computer network 34 and records any extra services used by a host computer network 34 and its authorized users. The fees for each particular host computer network are negotiated prior to beginning services to a particular host computer network and associated authorized users. The negotiated fees may be stored as tables in the ESS. The ESS 37 may be a server running UNIX software such as a SPARC Server available from SUN Microsystems. The ESS receives

updates on authorized users and subscribing host computer networks from the ISC.

A network management center (NMC) 39 is in communication with the ISC 35 and a private corporate intranet 19 via the ESS 37. The NMC 39 receives help requests from the ISC and provides a help desk for network infrastructure problems, performance issues and chronic desktop problems. The NMC 39 uses a pre-entered user definition and information to create a trouble record for resolving issues associated with remote access services provided to the host computer networks 34. Each trouble call is stored at the NMC 39. The NMC serves to provide proactive surveillance of all physical lines and routers in the system as well as handling trouble calls passed on from the ISC.

A customer service center (CSC) 40 is also linked to the system 10 via the ESS and the private corporate intranet 19. The CSC 40 manages the ordering of POTS services and repairs of business lines (e.g. DS1, ISDN, etc.). A billing application communicates over the corporate intranet 19, via the ESS 37, with the NAS 30 and other system 10 components to obtain necessary billing information concerning host computer networks 34 and their respective users. In one embodiment, the billing application is a software application running within the ESS containing logic necessary to organize cost data by per user and per entity within a particular client's (host computers) organization. Alternatively, the billing application may be a discrete billing computer 42 executing the necessary logic to obtain and manipulate billing information. A more detailed discussion of a method and system for monitoring computer usage and associated costs is discussed in a commonly assigned application identified as Attorney Docket No. 8285/142. That application is filed on the same date as the present application and is hereby incorporated by reference in its entirety.

As shown in FIG. 2, the communication server 20 preferably includes an internet protocol (IP) address memory 36 containing a list of source dial-in numbers and the appropriate IP address to direct calls received on specific dial-in numbers. In one embodiment, there are a plurality of communication

servers 20 that each service one specific host computer network 34 and hold the IP address for that specific host computer network in memory 36. In an alternative embodiment, one or more servers 20 each can direct authorized users to the appropriate one of several different host computer networks 34. The IP memory 36 also preferably includes the IP address of the service bureau 22. The communication server forwards calls received from the predetermined dial-in numbers to the IP address of the appropriate host computer network after the user is authorized by the NAS. Calls forwarded from remote computers 12 are converted from the POTS format to frame relay network messages in a frame relay translator 36 that converts the signals received from the frame relay network 24 or PSTN 18 to the appropriate format.

The NAS 30 communicates with the communication server 20 over the frame relay network 24 and authenticates each remote user's identification through a process of several steps. Referring to FIG. 3, a user name memory 38 in the NAS 30 contains user names for all authorized users of the various proprietary host computer networks 34 that utilize the services of the service bureau 22. A host computer IP address memory 42 contains a cross-referenced list of usernames and IP addresses of the computer or computers each username may have access to. The NAS also requires a pass code to authenticate a user. The pass code preferably consists of a fixed personal identification number (PIN) and a time variable security token password.

A secure identification generator 41 in the NAS 30 contains an algorithm for generating a unique security token password for each remote computer user. Each remote computer user has access to a personalized security token at her end of the remote call. The security token may be a soft token, such as a software application on each authorized user's computer, or a hard token, such as a secure identification card 14 available from Security Dynamics, Inc. of Cambridge, Massachusetts. Each authorized user's security token generates a unique security token password that may be a sequence of numbers, letters, or other type of symbol. Using the secure ID card 14, the security token password is obtained by the user from a display

showing a new security token password at predetermined time increments. The algorithm at the secure identification generator 41 is substantially synchronized with the encryption algorithm generating and displaying a security token password on the secure identification card 14 each user possesses. Thus, the NAS 30 and remote computer user share a unique, time variable security token password. The secure identification generator 41 may be a microprocessor implementing a time based security algorithm available from Security Dynamics, Inc. of Cambridge, Massachusetts, such as a 56 bit data encryption standard (DES).

Referring now to FIG. 4, a preferred embodiment of a method for securing communications between a remote user and a host computer network is illustrated. A user dials a telephone number with a computer modem 16, or other communications device, controlled by the user's computer. Preferably, the telephone number is a toll-free number so that the user may dial one number from any location to access her organization's host computer network via the communications server 20 and NAS 30. Each subscribing host computer network 34 has its own number or numbers, through a long distance service provider of its choice, that authorized users for that host computer network may use. The dialed number is received at the communication server to form a connection between remote user computer 12 and communication server 20 (at step 50). The connection is accomplished by routing the call from the modem 16 to the communication server over POTS lines 17, via the PSTN 18. Upon receipt of the call, the communication server establishes a connection with the NAS through the security service bureau 22 over the frame relay network.

When the communication server receives the call over the dial-in number, the user is queried for her user name. The user name may be any form of predetermined identification by which the host computer network recognizes the identity of a user registered on its system. In one embodiment, the communication server automatically prompts the remote user for her user name upon receipt of the remote user's call. The communication server then communicates this information to the NAS through

the frame relay network and service bureau. In another preferred embodiment, the communication server informs the NAS that a call has been received, and the NAS instructs the communication server to generate a user name prompt. The frame relay POTS translator 36 acts to properly format information flowing between the service bureau and user computer. Preferably, the communication server 20 and NAS 30 communicate using TCP/IP queries and transactions.

After receiving the remote user's response to the user name prompt, the communication server transmits the user name to the NAS. The NAS subsequently instructs the communication server to prompt the remote user for a pass code. The remote user enters the PIN and security token password that makes up her pass code and the communication server forwards the pass code, along with the IP address of the communication server 20, to the NAS (at steps 52, 54). Once the necessary information is entered, the NAS attempts to authenticate the user (at step 56). The NAS will only authenticate a user if certain conditions are met.

In one embodiment, each host computer network subscribing to the service bureau services has one corresponding communication server. The NAS first compares the entered user name to a list of usernames for the host computer network that corresponds with the received IP address of the communication server and retrieves the PIN number associated with the user name. The NAS will then generate a pass code that should match the particular remote user's time variant security token password and compare it with the one entered by the remote user. If the username and pass code entered by the user correspond exactly to those stored and generated at the NAS, the NAS transmits authorization for the communication server to link the remote user to the appropriate host computer network. In another embodiment, each communication server may be used with multiple host computer networks.

When the NAS transmits its authorization, the communication server determines the IP address of the proper host computer network by matching the remote user to the IP address associated with that user in the IP address

memory 34. Alternatively, the NAS may store the appropriate host computer network IP address in an IP address memory 42 and send the proper IP address with its authorization. The communication server then uses this address to establish a link to the proper host computer network over the frame relay network (at step 58). When the connection is made to the host computer network, the communication links for the session run from the remote user's computer 12 to the communication server 20 over the POTS lines, and from the communication server to the host computer network over the frame relay network.

The communication server records a starting time stamp and an ending time stamp for communication between the remote user and the host computer network. The starting and ending time stamps for each call, as well as other diagnostic information are periodically transmitted from the communication server to the service bureau The service bureau monitors the quality, frequency and duration of individual connections to each host computer network. The types of security measures taken by each host computer network, beyond the off-site authentication described above, are determined by each individual network according to the needs of the organization managing that network.

As has been described above, a system and method for providing remote computer users secure access to various unrelated, proprietary host computer networks is provided. The system and method reduce the need for duplication of efforts and dedication of extra resources by each host computer network by providing a security service bureau operated by a third party service provider that may operate the system to efficiently and securely manage authentication of users for each of the subscribing host computer networks. The service bureau NAS, in cooperation with one or more communication servers, handles authenticating a plurality of users to an appropriate one of a plurality of host computer networks and arranging for frame relay network connections to the user's respective host computer network. The method includes the steps of connecting remote users with a communication server and verifying a user's authenticity at a NAS with a user

name and pass code. As will be recognized by those skilled in the art, the type of computers and communications devices disclosed may be substituted for by any one of a number of commonly available computers and communications devices.

It is intended that the foregoing detailed description be regarded as illustrative rather than limiting, and that it be understood that the following claims, including all equivalents, are intended to define the scope of the invention.

WE CLAIM

1. A system for providing secure remote access between a host computer network and a remotely located computer, the system comprising:

a plurality of unrelated host computer networks, each host computer network having at least one user authorized to access information in the host computer network;

at least one communication server in communication with the host computer networks over a frame relay network;

a network access server in communication with the communication server over the frame relay network, the network access server having a memory, the memory comprising a list of host computer network user names and a secure identification algorithm for authenticating users seeking access to one of the host computer networks;

the communication server also in communication with at least one user computer via a communication network connection from the communication server to the user computer; and

a security token associated with a user at the user computer, the security token having a secure identification encryption algorithm identical to the secure identification encryption algorithm of the network access server and displaying a secure identification password for entry on the user computer.

2. The system of claim 1, wherein the at least one communication server comprises a plurality of communication servers, each of the communication servers in communication with the network access server and configured to communicate with a different one of the plurality of unrelated host computer networks, wherein all authorized users for a particular one of the plurality of unrelated host computer networks communicates through a single communication server.

3. The system of claim 1, wherein the at least one communication server comprises a plurality of communication servers, each of the communication servers in communication with the network access server and configured to communicate with a plurality of the unrelated host computer networks.

4. The system of claim 3, wherein the memory of the network access server further comprises a list of internet protocol (IP) addresses associated with the list of host computer network user names, whereby the network access server transmits an appropriate host computer network IP address for an authenticated user to the communication server.

5. The system of claim 3, wherein each communication server further comprises a host computer network IP address memory having a list of host computer network IP addresses associated with a list of host computer network usernames, whereby the communication server accesses an appropriate host computer network IP address for an authenticated user.

6. The system of claim 1 wherein the network access server is connected to a local area network.

7. The system of claim 1 wherein the user computer communicates with the communication server via a modem using a plain-old telephone system (POTS) connection.

8. The system of claim 1, wherein the communication network connection is a public switched telephone network (PSTN) connection.

9. The system of claim 7 wherein the modem communicates with the communication server on a toll free number.

10. The system of claim 1 wherein a modem call from a user authenticated by the network access server is connected in a communication path extending from the user computer to the communication server and from

the communication server to an appropriate one of the host computer networks over the frame relay network.

11. The system of claim 1, wherein the communication server comprises a memory containing a list of dialed telephone numbers associated with an internet protocol (IP) address for the network access server, whereby the communication server establishes a communication link with the network access server upon receipt of a call over a dialed number on the list of dialed numbers.

12. The system of claim 1, wherein the memory of the network access server further comprises a list of addresses for each of the plurality of host computer networks associated with a list of authorized users.

13. The system of claim 1, wherein the communication server is connected to a plurality of remotely located users, each of the remotely located users communicating with a different one of the plurality of host computer networks.

14. In a system having a plurality of unrelated host computer networks, each host computer network comprising at least one authorized user, at least one communication server configured to connect authorized users to a respective host computer network, and a network access server in communication with the communication server for controlling access to the host computer networks, a method of providing secure access to a host computer network comprising the steps of:

dialing a telephone number with a computer modem controlled by an authorized user's computer;

establishing a connection between the communication server and the authorized user's computer;

entering a user name at the authorized user's computer and transmitting the user name to a network access server via the communication server;

entering a pass code into the user's computer and transmitting the pass code to the network access server;

authenticating the user at the network access server based on the entered user name and pass code;

establishing a communication link between the user and a host computer network associated with the user via the communication server if the network access server authenticates the user.

15. The method of claim 14, wherein the step of dialing a telephone number with a computer modem comprises dialing a toll-free telephone number associated with the communication server over a plain old telephone service (POTS) telephone line.

16. The method of claim 15, wherein the telephone number links the user's computer to a communication server over the POTS line and the communication server establishes a communication link with the network access server over a frame relay network.

17. The method of claim 16, wherein the network access server comprises a memory containing internet protocol (IP) addresses for a plurality of host computer networks and the communication server establishes the communication link with the host computer network located at the IP address.

18. The method of claim 14, wherein the step of authenticating the user at the security server comprises the steps of comparing the user name received from the user with a list of users stored in the security server, and generating a pass code associated with the user name at the security server and comparing the pass code received from the user with the generated pass code.

19. The method of claim 14 wherein the step of establishing a communication link between the communication server and the host computer network comprises obtaining an internet protocol (IP) address for the host computer from the network access server and initiating the communication

link with the host computer network located at the obtained IP address, whereby the user is in communication with the host computer network via the communication server.

20. The method of claim 14, wherein the pass code comprises a fixed personal identification number and a time variable security token password.

21. A system for providing secure access between a plurality of host computer networks and a plurality of remotely located users comprising:

a security token associated with each of the plurality of remotely located users, the security token having password generating means for displaying a password to a user;

a user computer connected to communication means for communicating the password to a security service bureau;

the security service bureau having password generating means identical to the password generating means of the security token, the security service bureau further comprising means for authenticating each of the plurality of users to an appropriate one of the plurality of host computer networks and for authorizing a communication link between each user and the appropriate one of the host computer networks over a frame relay network.

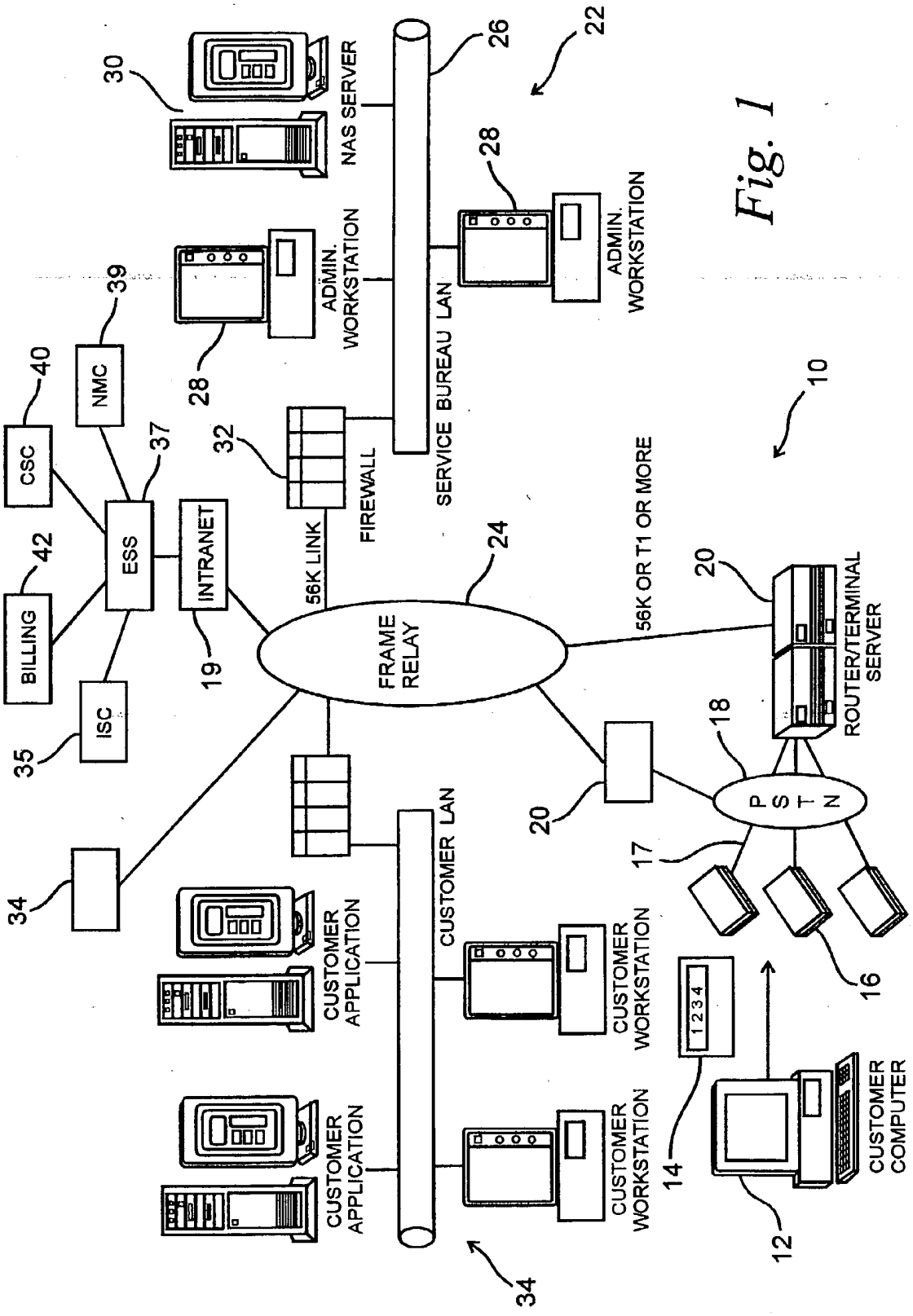


Fig. 1

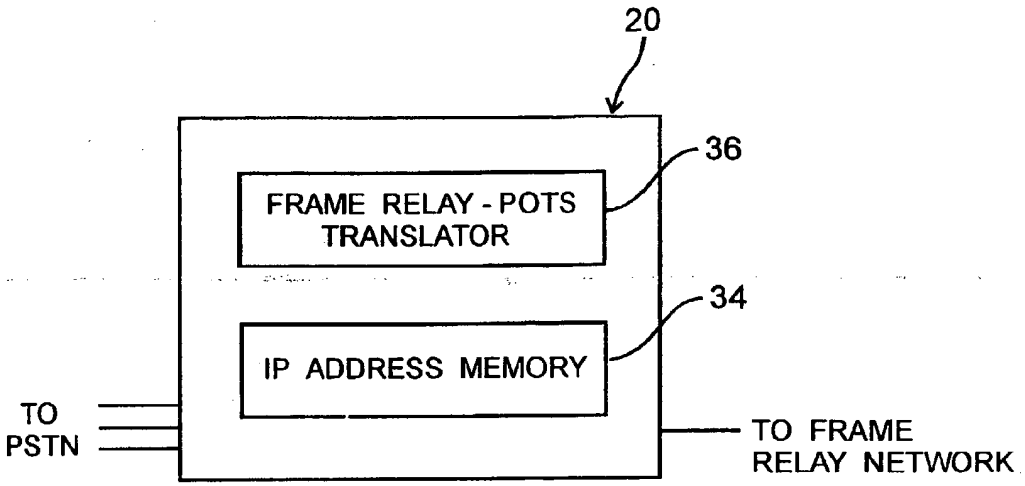


Fig. 2

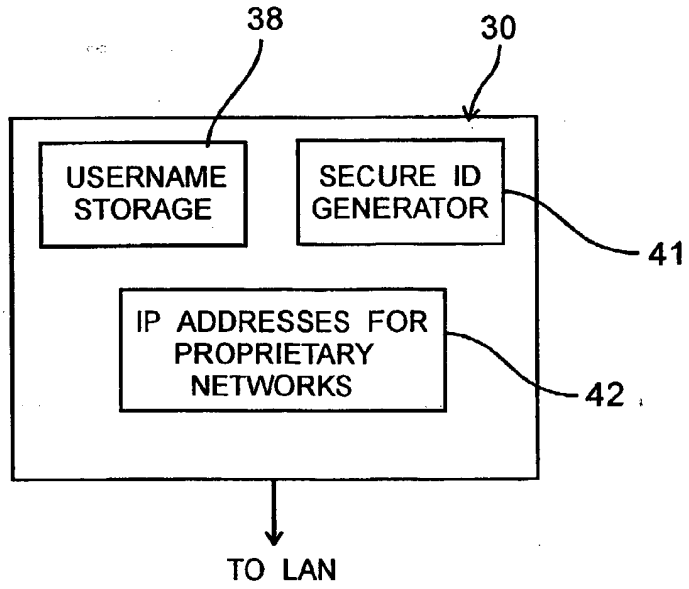


Fig. 3

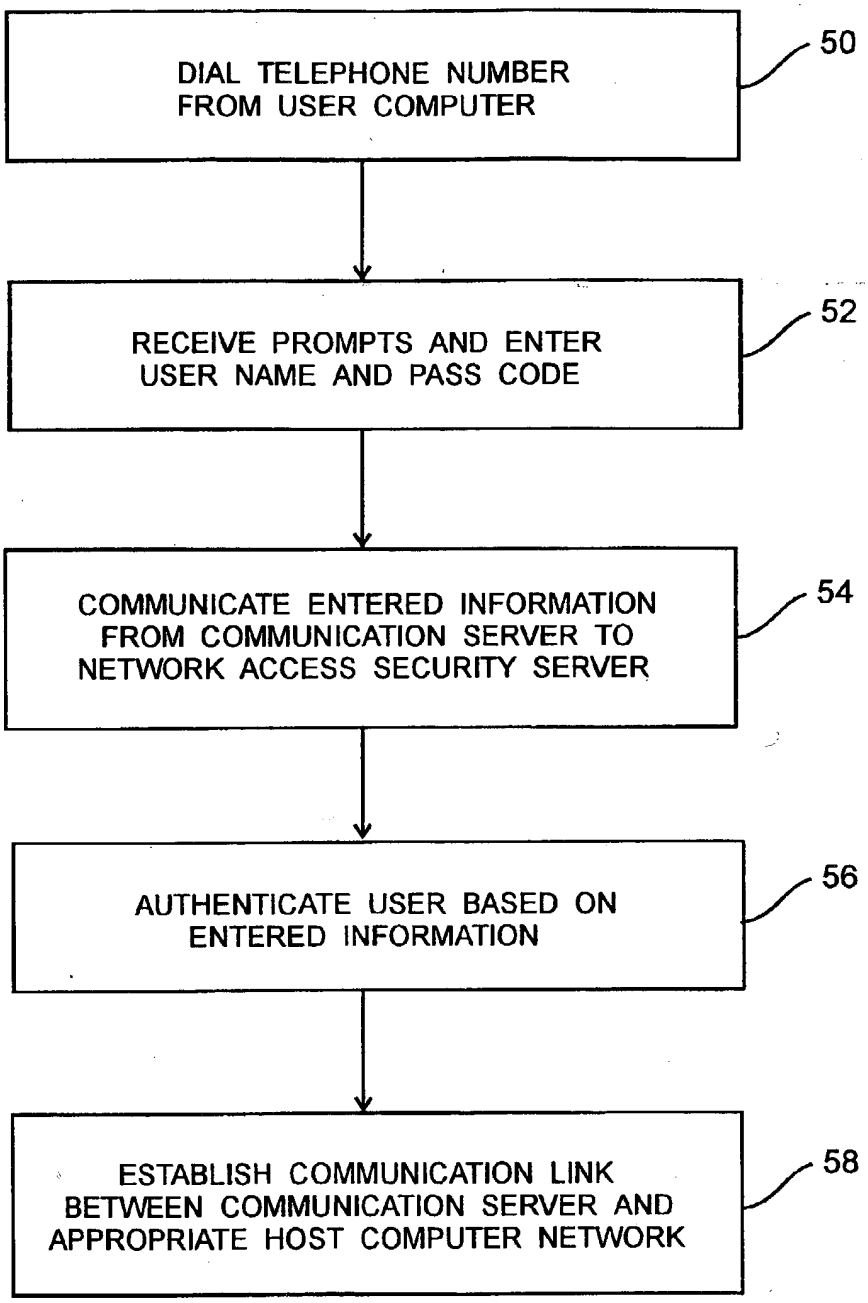


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/00778

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : H 04 L 9/32
US CL :380/23
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/23,25,49

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,661,807 A (GUSKI et al) 26 August 1997, abstract, col.6, lines 35-50, 57-67, col.7, lines 1-20, col.17, lines 55-60	1-21
Y	US 4,800,590 A (VAUGHAN) 24 January 1989, abstract, col.4, lines 2-21, 28-34, col.6, lines 33-44, col.7, lines 18-30, col.12, lines 16-17.	1-21
Y,E	US 5,867,494 A (KRISHNASWAMY et al) 02 February 1999, col.195, lines 63-67, col.196, lines 1-15, col.268, lines 60-67, col.269, lines 1-39.	1-21
Y,E	US 5,887,065 A (AUDEBERT) 23 March 1999, abstract, col.3, lines 30-50, col.6, lines 50-62, col.7, lines 4-9, col.17, lines 29-37.	1-21

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
01 APRIL 1999	16 APR 1999

Name and mailing address of the ISA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	GAIL HAYES
Facsimile No. (703) 305-0040	Telephone No. (703) 305-9711

Form PCT/ISA/210 (second sheet)(July 1992)*

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

APS
search terms: server, token,smart card, authentication,secret key, symmetric algorithm,encipher,encrypt,cipher, cypher, network,frame relay,internet protocol